Impossibility of Growing Quantum Bit Commitments

Severin Winkler
Computer Science Department, ETH Zurich, 8092 Zurich, Switzerland

Marco Tomamichel, Stefan Hengl, and Renato Renner
Institute for Theoretical Physics, ETH Zurich, 8093 Zurich, Switzerland

Quantum key distribution (QKD) is often, more correctly, called key growing. Given a short key as a seed, QKD enables two parties, connected by an insecure quantum channel, to generate a secret key of arbitrary length. Conversely, no key agreement is possible without access to an initial key. Here, we consider another fundamental cryptographic task, commitments. While, similar to key agreement, commitments cannot be realized from scratch, we ask whether they may be grown. That is, given the ability to commit to a fixed number of bits, is there a way to augment this to commitments to strings of arbitrary length? Using recently developed information-theoretic techniques, we answer this question in the negative.

Introduction.— Quantum key distribution [1, 2] allows two honest parties, Alice and Bob, to establish a shared secret key, using only insecure quantum communication. However, a necessary precondition for this to be possible is that they have access to a pre-shared initial key, to be used for authentication—a fact that is sometimes overlooked in the literature. It is easy to see that without such an initial key, it is impossible for Alice to distinguish between Bob and an eavesdropper pretending to be Bob — rendering all further security considerations futile. Nevertheless, once an initial key is available, this key can be *grown*, i.e., expanded to arbitrary length [3].

Another similar example is coin tossing. It is known that there is no unconditionally secure two-party protocol that generates a fair random coin which cannot be biased by a dishonest party [4]. However, if the two parties have access to a certain number of ideal coin tosses to start with, they can use protocols to obtain a larger number of secure coin tosses. (Here, security holds in a standalone model, where it is assumed that the protocol is invoked only once [5].)

Following this line of thought, one may wonder whether other cryptographic primitives, such as commitments [4], can be grown in a similar way. A *string commitment* protocol allows a sender to commit to a bit string that is revealed to a receiver at a later point. The protocol is secure for the sender (*hiding*) if the receiver cannot gain information about the commitment before she reveals it and it is secure for the receiver (*binding*) if the sender cannot change the string once committed. Here, we are only interested in unconditionally secure protocols, i.e., protocols that are secure against dishonest parties with unlimited computing power.

While it is known that unconditionally secure commitments cannot be implemented using classical or quantum communication only [6, 7] (see also [8, 9]), this Letter strives to answer the question whether it is possible to implement a long string commitment with a protocol that uses a smaller number of bit commitments that are provided as a resource. (A *bit commitment* is a string commitment of length one.) We will answer this question to the negative, showing that it is impossible to expand commitments even minimally, and even under relaxed security criteria.

Commitments have a wide variety of applications in theoretical cryptography, ranging from zero-knowledge proofs [10] to secure coin tossing. In particular, commitments can be used to implement statistically secure and universally composable oblivious transfer [11–13], a functionality that is sufficient to realize universal secure two-party computation [14].

In [15] it has been shown that unconditionally secure oblivious transfer cannot be extended using quantum protocols. We note that this already imposes certain bounds on the resources that can be obtained from a limited number of bit commitments [16]. Furthermore, bounds on the quality of commitments for relaxed security definitions have been shown in [17–19]. Conversely, it has been shown that secure commitments can be implemented in relativistic settings involving multiple sites [20] or using trusted resources such as a noisy channel [21] or (trusted) distributed randomness [22, 23].

We now proceed with a more detailed specification of string commitment as well as the class of protocols we consider. We then briefly review the smooth entropy calculus, which is required for our technical arguments. Our main result that commitments cannot be grown is stated as Theorem 1. This is supplemented with an alternative version of the claim, which applies if the initial functionality enables committing to quantum bits.

String Commitments.— A (classical) string commitment of length ℓ is a functionality that takes a bit string $x \in \{0,1\}^\ell$ from the sender and outputs the message `committed` to the receiver. Later, on input `open` from the sender, the functionality sends x to the receiver.

In the following, we consider implementations of this task by quantum protocols between two parties, Alice (who holds system A) and Bob (B). They have access to a noiseless quantum and a noiseless classical channel, as well as to an additional resource, C (to be specified

later). In any round of the protocol, the parties may perform an arbitrary quantum operation on the system in their possession conditioned on the available classical information [24] — this includes generating the input for the available communication interfaces. The use of the quantum channel then corresponds to a party transferring a part of her system to the other party. The classical channel measures the input in a canonical basis and sends the outcome to the receiver. We assume that the total number of rounds of the protocol is bounded by some finite number. By padding the protocol with empty rounds, this corresponds to the assumption that the number of rounds is equal in every execution.

A string commitment scheme over strings of length ℓ generally consists of two phases. In the first, the *commit phase*, the sender commits to an ℓ-bit string x. Later, in the *opening phase* the sender reveals x to the receiver. The total system (consisting of the subsystems controlled by Alice and Bob) is assumed to be in a pure state initially. By introducing an additional space the quantum operations of both parties can be purified, i.e., we can assume that the parties apply, conditioned on the information shared over the classical channel, isometries to their systems. Thus, we will assume in the following that the state at the end of the commit phase conditioned on all the classical communication is pure.

Security Definitions.— Our main technical contribution will be a quantitative statement on the impossibility of growing string commitments. To formulate this statement, we introduce two definitions that capture the cheating probability of Alice and the information gain of Bob, respectively. We emphasize that the properties required in these definitions are only necessary (we therefore call the definitions "weak"), but would not be sufficient for the security of a protocol [25]. Since we are interested in the impossibility of certain protocols, this only strengthens our results.

Using a commitment protocol, a (quantum) Alice can always commit to a superposition of strings [6, 26] as follows: she prepares a state $\frac{1}{\sqrt{|\mathcal{X}|}} \sum_{x\in\mathcal{X}} |x\rangle_X \otimes |x\rangle_{X'}$, where $\mathcal{X}$ is a subset of the ℓ-bit strings. Then she honestly executes the commit protocol with the first half of this state as input and keeps the system X'. We denote the resulting joint state of Alice, Bob and the resource system by $\rho^{\mathcal{X}}_{A'BC}$, where A' stands for $XX'A$. Later, Alice can measure X' and execute the opening phase of the protocol with the resulting string x. Thus, even for a perfectly binding commitment scheme, we cannot require that there is a fixed value x Alice is committed to after the commit phase. Rather, we can only demand that $\sum_{x\in\{0,1\}^n} p_x \leq 1$ where p_x is the probability that Alice successfully reveals some x in the opening phase.

In order to quantify the degree of bindingness of a protocol, we consider the following attack by Alice. First, she commits to a superposition of strings from a set $\mathcal{X}_0 \subseteq \{0,1\}^\ell$ as before. Then, she tries to map (by a local transformation $\mathcal{E}_A$ on her system) the resulting state $\rho^{\mathcal{X}_0}_{A'BC}$ to $\rho^{\mathcal{X}_1}_{A'BC}$, corresponding to the commitment to a set $\mathcal{X}_1 \subseteq \{0,1\}^\ell$ which is disjoint from $\mathcal{X}_0$. Such an attack is successful with probability at least Δ if the protocol cannot detect the transformation with probability more than $1-\Delta$. Using the *trace distance*, $D(\rho,\tau) := \frac{1}{2}\|\rho-\tau\|_1$, this can be turned into a necessary condition for security, formulated in terms of the closeness of the transformed state, $(\mathcal{E}_{A'} \otimes \mathbb{1}_{\mathrm{BC}})(\rho^{\mathcal{X}_0}_{A'BC})$, to the target state $\rho^{\mathcal{X}_1}_{A'BC}$.

Definition (Weakly Δ-binding)**.** We call a commitment scheme *weakly Δ-binding* if

$$\min_{\mathcal{X}_0,\mathcal{X}_1} \min_{\mathcal{E}_{A'}} D\left((\mathcal{E}_{A'} \otimes \mathbb{1}_{\mathrm{BC}})(\rho^{\mathcal{X}_0}_{A'BC}), \rho^{\mathcal{X}_1}_{A'BC}\right) \geq 1-\Delta \ ,$$

where $\mathcal{X}_0$ and $\mathcal{X}_1$ are disjoint sets of strings from $\{0,1\}^\ell$ and $\mathcal{E}_{A'}$ is a completely positive trace preserving map acting on Alice's system.

To define the hiding property, we consider the joint state ρ^x_{AB} of Alice's and Bob's systems that results from an execution of the protocol where both parties are honest and Alice commits to x. For a commitment scheme to be ε-hiding, we require that $D(\rho^x_B, \rho^{x'}_B) \leq \varepsilon$ for any x, x'. This immediately implies the following (necessary) security condition.

Definition (Weakly ε-hiding)**.** A bit commitment protocol is *weakly ε-hiding* for uniform X if the marginal state ρ_{XB} after the commit phase is ε-close to a state where X is uniform with respect to B, i.e.,

$$\min_{\sigma_B} D(\rho_{XB}, \frac{1}{|X|}\mathbb{1}_X \otimes \sigma_B) \leq \varepsilon \ . \tag{1}$$

Smooth Entropies.— Our proof is based on the insight that every conceivable protocol that aims to extend bit commitment allows for an attack, which can be established using known results on privacy amplification and the smooth entropy formalism. (Privacy amplification has also been used in [18] to construct attacks on commitment schemes.) The detailed proofs of the technical statements can be found in [27].

Let $\rho_{XB} = \sum_x P(x)|x\rangle\langle x| \otimes \rho^x_B$ be a classical-quantum (CQ) state. Then the min-entropy of X conditioned on B, denoted $H_{\min}(X|B)_\rho$, corresponds to the negative logarithm of the probability of guessing X correctly from a quantum memory B [28]. The smooth min-entropy of a state is defined as $H^\varepsilon_{\min}(X|B)_\rho := \max_{\tilde\rho} H_{\min}(X|B)_{\tilde\rho}$, where the optimization is over all (sub-normalized) states ε-close to ρ_{XB} in terms of the purified distance, which corresponds to the minimum trace distance between their purifications. The purified distance between two states, ρ and $\tilde\rho$, is upper bounded by $\sqrt{2D(\rho,\tilde\rho)}$ [29].

The *leftover hash lemma* against quantum side information [30] (see also [31]) asserts that the smooth min-entropy of $H^\varepsilon_{\min}(X|B)_\rho$ characterizes the amount of uniform randomness that can be extracted from X with

respect to the quantum side information B. A consequence of this is the following fact: for any CQ state $\rho_{XB} = \frac{1}{2^\ell}\sum_{x\in\{0,1\}^\ell} |x\rangle\langle x| \otimes \rho_B^x$ there exists a function $f : \{0,1\}^\ell \to \{0,1\}$ such that

$$D(\rho_B^{f,\mathcal{X}_0}, \rho_B^{f,\mathcal{X}_1}) \leq 2\epsilon + \sqrt{2^{1-H_{\min}^\varepsilon(X|B)_\rho}}\,, \qquad (2)$$

where $\rho_B^{f,\mathcal{X}_z} = \frac{1}{|f^{-1}(z)|}\sum_{x\in f^{-1}(z)} \rho_B^x$.

In order to derive bounds on the conditional min-entropy when the conditioning system is manipulated, we use the following data-processing inequalities. Let ρ_{XBC} be a CQ state, where C is an additional quantum register with dimension $|C|$. Then, the min-entropy $H_{\min}^\varepsilon(X|BC)_\rho$ cannot increase by more than $\log|C|$ when a projective measurement $C \to Z$ is applied,

$$H_{\min}^\varepsilon(X|BC)_\rho \geq H_{\min}^\varepsilon(X|BZ)_\rho - \log|C|\,. \qquad (3)$$

Moreover, if the classical register Z is discarded, we have

$$H_{\min}^\varepsilon(X|BZ)_\rho \geq H_{\min}^\varepsilon(X|B)_\rho - \log|Z|\,. \qquad (4)$$

The following fact, also used in the proofs of [6, 7, 32], is an essential building block of our impossibility proofs: let ϕ_{AB}^0 and ϕ_{AB}^1 be two pure states corresponding to the joint state of Alice and Bob when committing to '0' and '1', respectively. If the marginal state of ϕ_{AB}^0 and ϕ_{AB}^1 on Bob's system is (almost) the same, then there exists a unitary U_A on Alice system that (approximately) transforms ϕ_{AB}^0 into ϕ_{AB}^1, i.e., $(U_A \otimes \mathbb{1}_B)|\phi_{AB}^0\rangle \approx |\phi_{AB}^1\rangle$. This reasoning can be generalized to joint states ρ_{YAYB}^b that are pure conditioned on all the classical information Y available to both Alice and Bob as follows. If $D(\rho_{YB}^0, \rho_{YB}^1) \leq \varepsilon$, then there exists a unitary U_{YA} such that

$$D\big(U_{YA}\,\rho_{YAYB}^0\,U_{YA}^\dagger, \rho_{YAYB}^1\big) \leq \sqrt{2\varepsilon}\,, \qquad (5)$$

where we omitted the identity operator on YB.

Main Result— One can trivially implement a string commitment of length n from n bit commitments. Furthermore, it is easy to see that, using a resource which allows the parties to commit to n qubits, one can implement n individual commitments to two bits each using superdense coding [33], and, therefore, also a string commitment of length $2n$. Our main result essentially states that these two trivial implementations are essentially optimal.

More precisely, we first consider implementations of string commitments based on a functionality that enables n perfect (classical) bit commitments. We show that the length of the implemented string commitment is approximately upper bounded by n if this is required to be highly binding and hiding.

Theorem 1. *Every quantum protocol which uses n_A bit commitments from Alice to Bob and n_B bit commitments from Bob to Alice with $n = n_A + n_B$ as a resource and implements an ε-hiding and Δ-binding string commitment of length ℓ must satisfy*

$$\ell \leq n - 2\log\left(\frac{(1-\Delta)^2}{4} - \sqrt{2\varepsilon}\right) - 1\,.$$

In particular, if $\Delta = \varepsilon \leq 0.01$, then $\ell < n + 6$.

Proof. In the following, we construct an attack by Alice on a modified protocol that does not use the resource bit commitments and is not necessarily hiding. In this protocol we make Bob more powerful in the sense that he can simulate the original protocol locally. Thus, any successful attack of Alice against the modified protocol implies a successful attack against the original protocol.

In the modified protocol, Alice, instead of using the resource bit commitments, measures the bits to be committed, stores a copy and sends them to Bob, who stores them in a classical register, C_A. When one of these commitments is opened, he moves the corresponding bit to his register B. Bob simulates the action of his commitments locally as follows: instead of measuring a register, Y, and sending the outcome to the commitment functionality, he applies the isometry $U : |y\rangle_Y \mapsto |yy\rangle_{YY'}$ purifying the measurement of the committed bit and stores Y' in another register, C_B. When Bob has to open the commitment, he measures Y' and sends the outcome to Alice over the classical channel. Furthermore, the state conditioned on the classical communication is again pure.

Let $\rho_{XABC} = \frac{1}{2^\ell}\sum_x |x\rangle\langle x| \otimes \rho_{ABC}^x$, where C stands for C_AC_B, be the state resulting from the execution of the modified protocol when the input X of Alice is uniformly distributed. Its marginal state, ρ_{XAB}, is the corresponding state at the end of the commit phase of the original commitment protocol. The state ρ_{XB} must be weakly ε-hiding. Thus, by the definition of the smooth min-entropy and setting $\tilde{\varepsilon} := \sqrt{2\varepsilon}$, we get

$$H_{\min}^{\tilde{\varepsilon}}(X|B)_\rho \geq \log|X| = \ell. \qquad (6)$$

Therefore, inequalities (3) and (4) imply that

$$H_{\min}^{\tilde{\varepsilon}}(X|BC_AC_B)_\rho \geq H_{\min}^{\tilde{\varepsilon}}(X|B)_\rho - n \geq \ell - n\,. \qquad (7)$$

From (2) we know that there exists a function f such that $D(\rho_{BC}^{\mathcal{X}_0}, \rho_{BC}^{\mathcal{X}_1}) \leq 2\delta$, where $\delta := \tilde{\varepsilon} + \frac{1}{2}\sqrt{2^{1-H_{\min}^{\tilde{\varepsilon}}(X|BC)_\rho}}$ and $\rho_{BC}^{\mathcal{X}_z} = \frac{1}{|f^{-1}(z)|}\sum_{x\in f^{-1}(z)} \rho_{BC}^x$. In order to construct a concrete attack, let Alice choose a bit z and commit to a uniform superposition of all strings x with $f(x) = z$. Then the resulting joint state $\rho_{A'BC}^{\mathcal{X}_z}$ at the end of the commit phase is pure conditioned an all the shared classical information. According to (5) there exists, therefore, a unitary $U_{A'}$ on Alice's system that transforms $\rho_{A'BC}^{\mathcal{X}_z}$ into a state which is $2\sqrt{\delta}$-close to $\rho_{A'BC}^{\mathcal{X}_{1-z}}$ in terms of the trace distance. The definition of weakly Δ-binding implies that $1 - \Delta \leq 2\sqrt{\delta}$ and, together with (7), the statement follows. □

Next, we consider protocols which use a quantum commitment functionality that allows the parties to commit to (and later reveal) n qubit states. By slightly modifying the proof of the theorem, we show that there cannot exist a protocol that uses such a resource and implements a string commitment of length larger than $2n$. We consider again a modified protocol, where Bob simulates the resource system as follows: Alice, instead of using the resource, sends the committed qubits to Bob, and Bob keeps all the qubits that he would send to the commitment functionality in the original protocol in a register, C. Let ρ_{XABC} be the joint state after the execution of the commit phase when Alice's input X is uniformly distributed. We have $H_{\min}^{\tilde{\varepsilon}}(X|B)_\rho \geq \log|X| = \ell$ as in (6). Inequalities (3) and (4) together imply that conditioning on an additional quantum system C cannot decrease the smooth min-entropy by more than $2\log|C|$. Thus, we have

$$H_{\min}^{\tilde{\varepsilon}}(X|BC)_\rho \geq H_{\min}^{\tilde{\varepsilon}}(X|B)_\rho - 2\log|C| = \ell - 2n\ . \quad (8)$$

Now we proceed as in the proof of the main theorem to get

$$\ell \leq 2n - 2\log\left(\frac{(1-\Delta)^2}{4} - \sqrt{2\varepsilon}\right) - 1\ . \quad (9)$$

Note that the same reasoning applies to any resource which can be simulated by Bob such that the resulting state at the end of the commit phase is pure conditioned on all the classical communication and the simulated resource uses an additional memory of size at most $\log|C|$. Thus, inequality (9) holds for arbitrary such resources with $\log|C| \leq n$.

Conclusions— We proved that it is impossible to use a small number of bit commitments as a resource to implement a larger string commitment that is both arbitrarily binding and hiding. This is in stark contrast to corresponding positive results for other cryptographic primitives, such as *quantum key distribution* or *coin flipping*, where the resource of interest, once available in finite number, can be enlarged ad infinitum.

The techniques we use to show our impossibility results can be applied to prove more general results on the possibility and efficiency of two-party cryptography. In particular, they can be used to prove bounds on the efficiency of implementations of string commitments from oblivious transfer and, more generally, from resources that distribute trusted correlations to the parties. Moreover, the impossibility results on implementations of oblivious transfer presented in [15] can be improved using these techniques.

Acknowledgments.— We thank Frédéric Dupuis and Jürg Wullschleger for helpful and inspiring discussions. We acknowledge support from the Swiss National Science Foundation (grant no. 200020-135048), the European Research Council (grant no. 258932), and an ETH-IRA grant of ETH's research commission.

[1] C. H. Bennett and G. Brassard, in *Proc. IEEE Int. Conf. on Comp., Sys. and Signal Process.* (IEEE, Bangalore, 1984) pp. 175–179.
[2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (Aug 1991).
[3] An explicit calculation that shows that a constant-length initial key is sufficient to generate arbitrarily many novel key bits is given, for example, in [34].
[4] M. Blum, SIGACT News **15**, 23 (1983).
[5] D. Hofheinz, J. Müller-Quade, and D. Unruh, in *EUROCRYPT*, Lecture Notes in Computer Science, Vol. 4004, edited by S. Vaudenay (Springer, 2006) pp. 504–521.
[6] D. Mayers, Physical Review Letters **78**, 3414 (1997).
[7] H. K. Lo and H. F. Chau, Physical Review Letters **78**, 3410 (1997).
[8] G. M. D'Ariano, D. Kretschmann, D. Schlingemann, and R. F. Werner, Phys. Rev. A **76**, 032328 (Sep 2007).
[9] G. Chiribella, G. M. D'Ariano, P. Perinotti, D. M. Schlingemann, and R. F. Werner, ArXiv e-prints(May 2009), arXiv:0905.3801 [quant-ph].
[10] S. Goldwasser, S. Micali, and C. Rackoff, in *STOC* (ACM, 1985) pp. 291–304.
[11] C. H. Bennett, G. Brassard, C. Crépeau, and H. Skubiszewska, in *Advances in Cryptology — CRYPTO '91*, Lecture Notes in Computer Science, Vol. 576 (Springer, 1992) pp. 351–366.
[12] I. Damgård, S. Fehr, C. Lunemann, L. Salvail, and C. Schaffner, in *CRYPTO*, Lecture Notes in Computer Science, Vol. 5677, edited by S. Halevi (Springer, 2009) pp. 408–427.
[13] D. Unruh, in *EUROCRYPT*, Lecture Notes in Computer Science, Vol. 6110, edited by H. Gilbert (Springer, 2010) pp. 486–505.
[14] J. Kilian, in *Proceedings of the 20th Annual ACM Symposium on Theory of Computing (STOC '88)* (ACM Press, 1988) pp. 20–31.
[15] S. Winkler and J. Wullschleger, in *CRYPTO*, Lecture Notes in Computer Science, Vol. 6223, edited by T. Rabin (Springer, 2010) pp. 707–723.
[16] Using the equivalence of oblivious transfer and commitments, the result of [15] implies that there exists no *composable* protocol that implements $(m+1)$ *individual* bit commitments using m bit commitments as a resource, if one demands that the error decreases exponentially in m.
[17] R. W. Spekkens and T. Rudolph, Phys. Rev. A **65**, 012310 (Dec 2001).
[18] H. Buhrman, M. Christandl, P. Hayden, H.-K. Lo, and S. Wehner, Phys. Rev. Lett. **97**, 250501 (Dec 2006).
[19] A. Chailloux and I. Kerenidis, ArXiv e-prints(Feb. 2011), arXiv:1102.1678 [quant-ph].
[20] A. Kent, "Unconditionally secure bit commitment with flying qudits," (2011), arXiv:1101.4620.
[21] C. Crépeau, in *Advances in Cryptology — CRYPTO '97*, Lecture Notes in Computer Science, Vol. 1233 (Springer, 1997) pp. 306–317.
[22] H. Imai, J. Müller-Quade, A. Nascimento, and A. Winter, in *Proceedings of the IEEE International Symposium on Information Theory (ISIT '04)* (2004).
[23] S. Wolf and J. Wullschleger, in *Proceedings of 2004 IEEE Information Theory Workshop (ITW '04)* (2004).
[24] This assumption is not justified in the relativistic setting considered in [20].

[25] In particular, one would have to consider arbitrary malicious strategies of dishonest parties to prove the security of a protocol.
[26] P. Dumais, D. Mayers, and L. Salvail, in *EUROCRYPT*, Lecture Notes in Computer Science, Vol. 1807, edited by B. Preneel (LNCS, 2000) pp. 300–315.
[27] See EPAPS Document No.[number will be inserted by publisher].
[28] R. König, R. Renner, and C. Schaffner, Information Theory, IEEE Transactions on **55**, 4337 (sept. 2009), ISSN 0018-9448.
[29] M. Tomamichel, R. Colbeck, and R. Renner, IEEE Transactions on Information Theory **56**, 4674 (2010).
[30] R. Renner, Ph.D. thesis, ETH Zurich, (2005), arXiv: quant-ph/0512258.
[31] M. Tomamichel, R. Renner, C. Schaffner, and A. Smith, in *Information Theory Proceedings (ISIT), 2010 IEEE International Symposium on* (2010) pp. 2703 –2707.
[32] H. K. Lo, Physical Review A **56**, 1154 (1997).
[33] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (Nov 1992).
[34] J. Müller-Quade and R. Renner, New J. Phys. **11**, 085006 (Aug. 2009).
[35] C. A. Fuchs and J. van de Graaf, IEEE Transactions on Information Theory **45**, 1216 (1999).
[36] J. L. Carter and M. N. Wegman, Journal of Computer and System Sciences **18**, 143 (1979).

APPENDIX

Section A contains general definitions and technical lemmas related to distance measures and the smooth entropy calculus, as needed for our work. In Section B we present the full proofs of our main results.

A. Preliminaries

We restrict our attention to finite-dimensional Hilbert spaces $\mathcal{H}$. We use $\mathcal{P}(\mathcal{H})$ to denote the set of positive semi-definite operators on $\mathcal{H}$. We define the set of normalized quantum states by $\mathcal{S}_=(\mathcal{H}) := \{\rho \in \mathcal{P}(\mathcal{H}) : \operatorname{tr}\rho = 1\}$ and the set of sub-normalized states by $\mathcal{S}_\leq(\mathcal{H}) := \{\rho \in \mathcal{P}(\mathcal{H}) : 0 < \operatorname{tr}\rho \leq 1\}$. Given a state $\rho_{AB} \in \mathcal{S}_=(\mathcal{H}_\mathrm{A} \otimes \mathcal{H}_\mathrm{B})$ we denote by ρ_A and ρ_B its marginal states $\rho_A = \operatorname{tr}_\mathrm{B}(\rho_{AB})$ and $\rho_B = \operatorname{tr}_\mathrm{A}(\rho_{AB})$. We define the fidelity between two states $\rho, \tau \in \mathcal{S}_=(\rho)$ as $F(\rho,\tau) = \|\sqrt{\rho}\sqrt{\tau}\|_1$. For $\rho, \tau \in \mathcal{S}_=(\mathcal{H}_\mathrm{A})$, we define the *trace distance* between ρ and τ as

$$D(\rho,\tau) := \frac{1}{2}\|\rho - \tau\|_1.$$

For $b \in \{0,1\}$, let $\rho^b_{XB} = \sum_x |x\rangle\langle x| \otimes \rho_B^{x,b}$ be classical-quantum (CQ) states. Then we have (see [30] for a proof)

$$\|\rho^0_{XB} - \rho^1_{XB}\|_1 = \sum_{x\in\mathcal{X}} \|\rho_B^{x,0} - \rho_B^{x,1}\|_1. \tag{10}$$

Definition 2. For $\rho_{AB} \in \mathcal{S}_=(\mathcal{H}_{\mathrm{AB}})$ we define the *distance from uniform of A conditioned on B* as

$$\Delta(A|B)_\rho := \min_{\sigma_B} \; D(\rho_{AB}, \omega_A \otimes \sigma_B)\,, \tag{11}$$

where $\omega_A := \mathbb{1}_\mathrm{A}/\dim\mathcal{H}_\mathrm{A}$ and the minimum is taken over all $\sigma_B \in \mathcal{S}_=(\mathcal{H}_\mathrm{B})$.

Lemma 3. *Let $\rho_{XB} = \sum_{x\in\{0,1\}} \frac{1}{2}|x\rangle\langle x| \otimes \rho_B^x$ be a CQ state and $\Delta(X|B)_\rho \leq \varepsilon$. Then*

$$D(\rho^0_B, \rho^1_B) \leq 2\varepsilon.$$

Proof. $D(\rho_{XB}, \omega_A \otimes \sigma_B) \leq \varepsilon$ implies

$$\|\rho^0_B - \rho^1_B\|_1 \leq \|\rho^0_B - \sigma_B\|_1 + \|\rho^1_B - \sigma_B\|_1 \leq 4\varepsilon$$

where we used (10) and, therefore, we have $D(\rho^0_B, \rho^1_B) \leq 2\varepsilon$. □

Furthermore, we will make use of the following well-known technical lemma which is also used in [6, 7, 32].

Lemma 4. *Let $|\psi^0_{AB}\rangle$ and $|\psi^1_{AB}\rangle$ be states with $D(\rho^0_B, \rho^1_B) \leq \varepsilon$ where $\rho^x_B = \operatorname{tr}_\mathrm{A}|\psi^x_{AB}\rangle\langle\psi^x_{AB}|$. Then there exists a unitary U_A such that*

$$D(|\phi^1_{AB}\rangle\langle\phi^1_{AB}|, |\psi^1_{AB}\rangle\langle\psi^1_{AB}|) \leq \sqrt{2\varepsilon}$$

with $\phi^1_{AB} = (U_A \otimes \mathbb{1}_\mathrm{B})|\psi^0_{AB}\rangle$.

Proof. $D(\rho_B^0, \rho_B^1) \leq \varepsilon$ implies $F(\rho_B^0, \rho_B^1) \geq 1-\varepsilon$. From Uhlmann's theorem we know that there exists a unitary U_A such that $F(|\phi_{AB}^1\rangle\langle\phi_{AB}^1|, |\psi_{AB}^1\rangle\langle\psi_{AB}^1|) \geq 1-\varepsilon$ where $|\phi_{AB}^1\rangle = (U_A \otimes \mathbb{1}_{\mathrm{B}})|\psi_{AB}^0\rangle$. Since $D(\rho,\tau) \leq \sqrt{1-F(\rho,\tau)^2}$ for any $\rho, \tau \in \mathcal{S}_=(\mathcal{H})$ [35], we have $\sqrt{1-D(|\phi_{AB}^1\rangle\langle\phi_{AB}^1|, |\psi_{AB}^1\rangle\langle\psi_{AB}^1|)^2} \geq 1-\varepsilon$. Hence,

$$D(|\phi_{AB}^1\rangle\langle\phi_{AB}^1|, |\psi_{AB}^1\rangle\langle\psi_{AB}^1|) \leq \sqrt{1-(1-\varepsilon)^2} \leq \sqrt{2\varepsilon}$$

□

Lemma 4 can be generalized to states which are pure conditioned on all classical information available to both A and B in the following way.

Lemma 5. *For $b \in \{0,1\}$, let*

$$\rho_{XX'AB}^b = \sum_x P_b(x)|x\rangle\langle x|_X \otimes |x\rangle\langle x|_{X'} \otimes |\psi_{AB}^{x,b}\rangle\langle\psi_{AB}^{x,b}|$$

with $D(\rho_{X'B}^0, \rho_{X'B}^1) \leq \varepsilon$. Then there exists a unitary U_{AX} such that

$$D(\rho_{XX'AB}'^1, \rho_{XX'AB}^1) \leq 2\varepsilon$$

where $\rho_{XX'AB}'^1 = (U_{XA} \otimes \mathbb{1}_{X'B})\rho_{XX'AB}^0(U_{XA} \otimes \mathbb{1}_{X'B})^\dagger$.

Proof. Define $|\psi_{XX'X''AB}^b\rangle := \sum_x \sqrt{P_b(x)}|x\rangle_X \otimes |x\rangle_{X'} \otimes |x\rangle_{X''} \otimes |\psi_{AB}^{x,b}\rangle$ and let

$$\rho_{X'X''B}^b = \mathrm{tr}_{\mathrm{XA}}(|\psi_{XX'X''AB}^b\rangle\langle\psi_{XX'X''AB}^b|).$$

Then

$$D(\rho_{X'X''B}^0, \rho_{X'X''B}^1) = D(\rho_{X'B}^0, \rho_{X'B}^1) \leq \varepsilon$$

Thus, Lemma 4 implies the existence of a unitary U_{AX} such that

$$D(|\phi_{XX'X''AB}^1\rangle\langle\phi_{XX'X''AB}^1|, |\psi_{XX'X''AB}^1\rangle\langle\psi_{XX'X''AB}^1|) \leq \sqrt{2\varepsilon}$$

with $|\phi_{XX'X''AB}^1\rangle = (U_{AX} \otimes \mathbb{1}_{X'X''B})|\psi_{XX'X''AB}^0\rangle$. The statement then follows from the fact that taking the partial trace over X'' cannot increase the trace distance and commutes with the unitary U_{AX} as follows. Let $\rho_{XX'AB}'^1 = (U_{XA} \otimes \mathbb{1}_{X'B})\rho_{XX'AB}^0(U_{XA} \otimes \mathbb{1}_{X'B})^\dagger$. Then

$$\begin{aligned}
&D((U_{XA} \otimes \mathbb{1}_{X'B})\rho_{XX'AB}^0(U_{XA} \otimes \mathbb{1}_{X'B})^\dagger, \rho_{XX'AB}^1) \\
&\quad = D((U_{XA} \otimes \mathbb{1}_{X'B})\mathrm{tr}_{\mathrm{X''}}(\rho_{XX'X''AB}^0)(U_{XA} \otimes \mathbb{1}_{X'B})^\dagger, \mathrm{tr}_{\mathrm{X''}}(\rho_{XX'X''AB}^1)) \\
&\quad = D(\mathrm{tr}_{\mathrm{X''}}((U_{XA} \otimes \mathbb{1}_{X'X''B})\rho_{XX'X''AB}^0(U_{XA} \otimes \mathbb{1}_{X'X''B})^\dagger), \mathrm{tr}_{\mathrm{X''}}(\rho_{XX'X''AB}^1)) \\
&\quad \leq D((U_{XA} \otimes \mathbb{1}_{X'X''B})\rho_{XX'X''AB}^0(U_{XA} \otimes \mathbb{1}_{X'X''B})^\dagger, \rho_{XX'X''AB}^1) \\
&\quad \leq \sqrt{2\varepsilon}
\end{aligned}$$

□

We define the non-smooth min-entropy as follows.

Definition 6 (Min-Entropy)**.**

$$H_{\min}(A|B)_\rho := \max_{\sigma_B \in \mathcal{S}_=(\mathcal{H}_{\mathrm{B}})} \sup\left\{\lambda \in \mathbb{R} : 2^{-\lambda}\,\mathbb{1}_{\mathrm{A}} \otimes \sigma_B \geq \rho_{AB}\right\}.$$

Then we define the smooth version of the min-entropy of a state ρ as an optimization of the non-smooth entropy over a set of states that are close to ρ. As a distance measure between two states we use the purified distance, which corresponds to the minimum trace distance between purifications of these states [29].

Definition 7 (Purified Distance)**.** For $\rho, \tau \in \mathcal{S}_\leq(\mathcal{H})$, we define the *purified distance* between ρ and τ as

$$P(\rho,\tau) := \sqrt{1-\bar{F}(\rho,\tau)^2}$$

where the generalized fidelity $\bar{F}$ is defined as $\bar{F}(\rho,\tau) = F(\rho,\tau) + \sqrt{(1-\mathrm{tr}\,\rho)(1-\mathrm{tr}\,\tau)}$. Note that $\bar{F}(\rho,\tau) = F(\rho,\tau)$ if at least one of the states is normalized.

Let $\varepsilon \geq 0$ and $\rho \in \mathcal{S}_{\leq}(\mathcal{H})$ with $\sqrt{\operatorname{tr}\rho} > \varepsilon$. Then, we define an *$\varepsilon$-ball* in $\mathcal{H}$ around ρ as

$$\mathcal{B}^{\varepsilon}(\mathcal{H};\rho) := \{\tau \in \mathcal{S}_{\leq}(\mathcal{H}) : P(\tau,\rho) \leq \varepsilon\}.$$

The smoothed version of the min-entropy is defined as follows.

Definition 8 (Smooth Min-Entropy)**.** Let $\varepsilon \geq 0$ and $\rho_{AB} \in \mathcal{S}_{\leq}(\mathcal{H}_{\mathrm{AB}})$, then the *$\varepsilon$-smooth min-entropy* of A conditioned on B of ρ_{AB} is defined as

$$H_{\min}^{\varepsilon}(A|B)_{\rho} := \max_{\tilde{\rho}_{AB} \in \mathcal{B}^{\varepsilon}(\rho_{AB})} H_{\min}(A|B)_{\tilde{\rho}}.$$

A family $\mathcal{F}$ of functions from $\mathcal{X}$ to $\mathcal{Z}$ is called weakly two-universal [36] if for any pair of distinct inputs x and x' the probability of a collision $f(x) = f(x')$ is at most $1/|\mathcal{Z}|$ if f is chosen at random from $\mathcal{F}$. The following lemma [30] (see also [31]) shows that weak two-universal hash functions are strong extractors against quantum side information, i.e., the output of the function is uniform with respect to the side information and the choice of the function.

Lemma 9 (Leftover Hash Lemma)**.** *Let $\mathcal{F}$ be a family of weak two-universal hash functions from $\mathcal{X}$ to $\{0,1\}$. Let $\rho_{XB} = \sum_x P(x)|x\rangle\langle x| \otimes \rho_B^x$ be a CQ state and $\rho_{FZB} = \frac{1}{|\mathcal{F}|}\sum_f \sum_z |f\rangle\langle f| \otimes |z\rangle\langle z| \otimes \rho_B^{f,z}$ with $z \in \{0,1\}$ and $\rho_B^{f,z} = \sum_{x \in f^{-1}(z)} P(x)\rho_B^x$. Then*

$$\Delta(Z|BF)_{\rho} \leq \epsilon + \frac{1}{2}\sqrt{2^{1-H_{\min}^{\varepsilon}(X|B)_{\rho}}}.$$

Lemma 10. *Let $\rho_{XB} = \frac{1}{2^{\ell}}\sum_{x\in\{0,1\}^{\ell}} |x\rangle\langle x| \otimes \rho_B^x$ be a CQ state. Then there exists a function $f : \{0,1\}^{\ell} \to \{0,1\}$ in $\mathcal{F}$ such that*

$$D(\rho_B^{f,0}, \rho_B^{f,1}) \leq 2\left(\epsilon + \frac{1}{2}\sqrt{2^{1-H_{\min}^{\varepsilon}(X|B)_{\rho}}}\right),$$

where $\rho_B^{f,z} = \frac{1}{|f^{-1}(z)|}\sum_{x\in f^{-1}(z)} \rho_B^x$.

Proof. Let $\mathcal{F}$ be a family of two-universal hash functions $f : \{0,1\}^{\ell} \to \{0,1\}$ such that every f is balanced, i.e., $|\{x \in \{0,1\}^{\ell} : \ f(x) = 0\}| = 2^{\ell-1}$. From Lemma 9 we know that

$$\Delta(Z|BCF)_{\rho} \leq \delta$$

where $\delta := \varepsilon + \frac{1}{2}\sqrt{2^{1-H_{\min}^{\varepsilon}(X|B)_{\rho}}}$ and $Z := f(X)$. Thus, there must exist a function $f \in \mathcal{F}$ such that $\Delta(Z|B)_{\rho^{[f]}} \leq \delta$. For $z \in \{0,1\}$ let

$$\rho_B^{f,z} = \frac{1}{2^{\ell-1}} \sum_{x \in f^{-1}(z)} \rho_B^x.$$

From Lemma 3 we then have $D(\rho_{BC}^{f,0}, \rho_{BC}^{f,1}) \leq 2\delta$. □

The following lemma shows that the conditional min-entropy $H_{\min}^{\varepsilon}(A|B)_{\rho}$ can decrease by at most $\log|Z|$ when conditioning on an additional classical system Z.

Lemma 11. *Let $\varepsilon > 0$ and let ρ_{ABZ} be a tripartite state that is classical on Z with respect to some orthonormal basis $\{|z\rangle\}_z$. Then*

$$H_{\min}^{\varepsilon}(A|BZ)_{\rho} \geq H_{\min}^{\varepsilon}(A|B)_{\rho} - \log|Z|.$$

Proof. Let $\tilde{\rho}_{AB}$ be the state that optimizes the min-entropy $H_{\min}^{\varepsilon}(A|B)_{\rho} = H_{\min}(A|B)_{\tilde{\rho}}$. Then, there exists an extension $\tilde{\rho}_{ABZ}$ of $\tilde{\rho}_{AB}$ that is ε-close to ρ_{ABZ} and classical on Z. See [29], where it is shown that there always exists an ε-close extension and that the purified distance can only decrease under a measurement in the Z basis. Let $\tilde{\rho}_{ABZ} = \sum_z \tilde{\rho}_{AB}^z \otimes |z\rangle\langle z|$ so that $\tilde{\rho}_{AB}^z \leq \tilde{\rho}_{AB}$ for all z. By the definition of the min-entropy, we have

$$\tilde{\rho}_{AB}^z \leq \tilde{\rho}_{AB} \leq 2^{-H_{\min}^{\varepsilon}(A|B)} \mathbb{1}_{\mathrm{A}} \otimes \sigma_B$$

for the optimal σ_B. Hence,

$$\tilde{\rho}_{ABC} = \sum \tilde{\rho}_{AB}^z \otimes |z\rangle\langle z| \leq 2^{-H_{\min}^{\varepsilon}(A|B)} \mathbb{1}_{\mathrm{A}} \otimes \sigma_B \otimes \mathbb{1}_{\mathrm{Z}}.$$

The lemma now follows from the definition of the min-entropy $H_{\min}^{\varepsilon}(A|BZ)_{\rho}$, where $\tilde{\rho}_{ABZ}$ and $\sigma_{BZ} = \sigma_B \otimes \mathbb{1}_{\mathrm{Z}}/|\mathrm{Z}|$ are candidates for the optimization. □

The following lemma shows that the min-entropy $H_{\min}^{\varepsilon}(A|BC)_\rho$ cannot increase too much when a projective measurement is applied to system C.

Lemma 12. *Let $\varepsilon \geq 0$ and let ρ_{ABC} be a tri-partite state. Furthermore, let $\mathcal{M}$ be a projective measurement in the basis $\{|z\rangle\}_z$ on C and $\rho_{ABZ} := \mathcal{I}_{AB} \otimes \mathcal{M}(\rho_{ABC})$, where $\mathcal{I}_{AB}$ is the identity operation on A and B. Then,*

$$H_{\min}^{\varepsilon}(A|BC)_\rho \geq H_{\min}^{\varepsilon}(A|BZ)_\rho - \log|\mathrm{Z}|\,.$$

Proof. Let $U : |z\rangle_{\mathrm{C}} \mapsto |zz\rangle_{\mathrm{ZZ'}}$ be the isometry purifying $\mathcal{M}$ in the sense that $\rho_{ABZ} = \mathrm{tr}_{\mathrm{Z'}}(\rho_{ABZZ'})$, where $\rho_{ABZZ'} := U\rho_{ABC}U^\dagger$. Covariance under isometries of the smooth min-entropy implies

$$H_{\min}^{\varepsilon}(A|BC)_\rho = H_{\min}^{\varepsilon}(A|BZZ')_\rho\,.$$

Moreover, for some states $\tilde{\rho}_{ABZ}$ and $\tilde{\sigma}_{BZ}$, we have

$$\begin{aligned} H_{\min}^{\varepsilon}(A|BZ)_\rho &= \sup\left\{\lambda \in \mathbb{R} : \tilde{\rho}_{ABZ} \leq 2^{-\lambda}\,\mathbb{1}_{\mathrm{A}} \otimes \tilde{\sigma}_{BZ}\right\} \\ &\leq \sup\left\{\lambda \in \mathbb{R} : \tilde{\rho}_{ABZZ'} \leq 2^{-\lambda}\,|\mathrm{Z}|\,\mathbb{1}_{\mathrm{A}} \otimes \tilde{\sigma}_{BZZ'}\right\} \\ &\leq H_{\min}^{\varepsilon}(A|BZZ')_\rho + \log|\mathrm{Z}|\,. \end{aligned} \tag{12}$$

Here, $\tilde{\rho}_{ABZZ'}$ is an extension of $\tilde{\rho}_{ABZ}$ that is ε-close to $\rho_{ABZZ'}$ and satisfies $\Pi_{ZZ'}\tilde{\rho}_{ABZZ'}\Pi_{ZZ'} = \tilde{\rho}_{ABZZ'}$, where $\Pi_{ZZ'} := \sum_z |zz\rangle\langle zz|_{\mathrm{ZZ'}}$. The existence of such an extension can be deduced from the fact that projections can only decrease the purified distance [29] and $\Pi_{ZZ'}$ commutes with $\rho_{ABZZ'}$. Furthermore, $\tilde{\sigma}_{BZZ'} := \Pi_{ZZ'}(\tilde{\sigma}_{BZ} \otimes \mathbb{1}_{\mathrm{Z'}})\Pi_{ZZ'}$. The last inequality follows since $\tilde{\rho}_{ABZZ'}$ and $\tilde{\sigma}_{BZZ'}$ are candidates for the optimization of the min-entropy. It remains to show the implication

$$\tilde{\rho}_{ABZ} \leq 2^{-\lambda}\,\mathbb{1}_{\mathrm{A}} \otimes \tilde{\sigma}_{BZ} \implies \tilde{\rho}_{ABZZ'} \leq 2^{-\lambda}\,|\mathrm{Z}|\,\mathbb{1}_{\mathrm{A}} \otimes \tilde{\sigma}_{BZ} \otimes \mathbb{1}_{\mathrm{Z'}} \tag{13}$$

which in turn implies (12). However, (13) follows from the fact that, for any extension X_{AB} of a positive operator X_A, it holds that $X_{AB} \leq |\mathrm{B}|\,X_A \otimes \mathbb{1}_{\mathrm{B}}$. Since X_{AB} has a spectral decomposition with positive coefficients, it is sufficient to show this property for pure normalized states $|\psi\rangle\langle\psi|_{\mathrm{AB}}$. The general property then follows by taking the weighted sum on both sides of the inequality. Let $\tau_A := \mathrm{tr}_{\mathrm{B}}(|\psi\rangle\langle\psi|_{\mathrm{AB}})$ and $\Gamma_{AB} := (\tau_A^{-\frac{1}{2}} \otimes \mathbb{1}_{\mathrm{B}})|\psi\rangle\langle\psi|_{\mathrm{AB}}\,(\tau_A^{-\frac{1}{2}} \otimes \mathbb{1}_{\mathrm{B}})$, where the inverse is taken on the support of τ_A. Since Γ_{AB} is of rank 1, its maximum eigenvalue is $\mathrm{tr}(\Gamma_{AB}) = \mathrm{rank}\{\tau_A\} \leq \min\{|\mathrm{A}|, |\mathrm{B}|\}$ and, thus, $\Gamma_{AB} \leq |\mathrm{B}|\,\mathbb{1}_{\mathrm{AB}}$. Hence, by conjugation of both sides with $\tau_A^{\frac{1}{2}}$ follows $|\psi\rangle\langle\psi|_{\mathrm{AB}} \leq |\mathrm{B}|\,\tau_A \otimes \mathbb{1}_{\mathrm{B}}$. This concludes the proof. □

The following lemma, which shows that conditioning on an additional quantum system C cannot decrease the conditional smooth min-entropy by more than $2\log|C|$, follows immediately from Lemmas 11 and 12

Lemma 13. $H_{\min}^{\varepsilon}(A|BC)_\rho \geq H_{\min}^{\varepsilon}(A|B)_\rho - 2\log|C|$.

B. Main Results

(Classical) Bit Commitment Resource

Theorem 14. *Every quantum protocol which uses n_A (classical) bit commitments from Alice to Bob and n_B (classical) bit commitments from Bob to Alice with $n = n_A + n_B$ as a resource and implements an ε-hiding and Δ-binding string commitment of length at most*

$$\ell \leq n - 2\log\left(\frac{(1-\Delta)^2}{4} - \sqrt{2\varepsilon}\right) - 1.$$

In particular, if $\Delta = \varepsilon \leq 0.01$, then $\ell \leq n + 6$.

Proof. Let $|x\rangle\langle x| \otimes \rho_{ABC}^x$ be the state resulting from the execution of an ε-hiding commitment protocol when the input of Alice is x. Then $\rho_{XABC} = \sum_x \frac{1}{2^\ell}|x\rangle\langle x| \otimes \rho_{ABC}^x$ is the state resulting from an execution where the committed string X is uniformly distributed. Let $\tilde{\varepsilon} := \sqrt{2\varepsilon}$. Since ρ_{XB} is ε-close to uniform and $P(\rho, \rho') \leq \sqrt{2D(\rho, \rho')}$ [29], the definition of the smooth min-entropy implies that

$$H_{\min}^{\tilde{\varepsilon}}(X|B)_\rho \geq \log|X| = \ell.$$

In the following, we consider a modified protocol that does not use the resource bit commitments. In this modified protocol Alice, instead of using the resource bit commitments, measures the bits to be committed, stores a copy and sends them to Bob, who stores them in a classical register C_A. When one of these commitments is opened, he moves the coresponding bit to his register B. Bob simulates the action of his commitments locally as follows: instead of measuring a register, Y, and sending the outcome to the commitment functionality, he applies the isometry $U : |y\rangle_Y \mapsto |yy\rangle_{YY'}$ purifying the measurement of the committed bit and stores Y' in register C_B. When Bob has to open the commitment, he measures Y' and sends the outcome to Alice over the classical channel. Note that we make Bob more powerful in this modified protocol because he can simulate the original protocol locally. Thus, any successful attack of Alice against the modified protocol implies a successful attack against the original protocol. Since we only make use of the modified protocol to construct an attack against Bob, the modified protocol does not have to be hiding. Furthermore, the state conditioned on the classical communication is again pure. Let $|x\rangle\langle x| \otimes \bar{\rho}^x_{AB}$ be the state resulting from the execution of the modified protocol when the input of Alice is x. Then $\bar{\rho}_{XAB} = \sum_x \frac{1}{2^\ell} |x\rangle\langle x| \otimes \bar{\rho}^x_{AB}$ is the state resulting from an execution where the committed string X is uniformly distributed. From Lemma 10 we know that there exists a function $f : \{0,1\}^\ell \to \{0,1\}$ such that

$$D(\rho^{\mathcal{X}_0}_{BC}, \rho^{\mathcal{X}_1}_{BC}) \leq 2\delta$$

where $\rho^{\mathcal{X}_z}_{BC} = \frac{1}{2^{\ell-1}} \sum_{x \in f^{-1}(z)} \rho^x_{BC}$, $\delta := \tilde{\varepsilon} + \frac{1}{2}\sqrt{2^{1-H^{\tilde{\varepsilon}}_{\min}(X|BC)_\rho}}$ and C stands for C_AC_B. Let $z \in \{0,1\}$ and let Alice prepare the state

$$\frac{1}{\sqrt{2^{\ell-1}}} \sum_{x \in f^{-1}(z)} |x\rangle_X \otimes |x\rangle_{X'}$$

and honestly executes the commit protocol with the first half of this state as input. Let $\rho^{\mathcal{X}_z}_{A'BC_AC_B} = \rho^{\mathcal{X}_z}_{XX'ABC_AC_B}$ be the resulting joint state at the end of the commit phase. Then we have $\mathrm{tr}_{\mathrm{A}'}(\rho^{\mathcal{X}_z}_{A'BC_AC_B}) = \rho^{\mathcal{X}_z}_{BC_AC_B}$ and, therefore, Lemma 5 then implies that there exists unitary U_A such that

$$D(\tilde{\rho}^{\mathcal{X}_z}_{A'BC_AC_B}, \rho^{\mathcal{X}_z}_{A'BC_AC_B}) \leq 2\sqrt{\delta}, \tag{14}$$

where $\tilde{\rho}^{\mathcal{X}_z}_{A'BC_AC_B} = (U_{A'} \otimes \mathbb{1}_{\mathrm{B}})\rho^{\mathcal{X}_z}_{A'BC_AC_B}(U_{A'} \otimes \mathbb{1}_{\mathrm{B}})^\dagger$. Lemmas 11 and 12 imply that

$$\begin{aligned} H^{\tilde{\varepsilon}}_{\min}(X|BC_AC_B)_\rho &\geq H^{\tilde{\varepsilon}}_{\min}(X|BC_B)_\rho - n_A \\ &\geq H^{\tilde{\varepsilon}}_{\min}(X|B)_\rho - n \\ &\geq \ell - n \end{aligned} \tag{15}$$

Thus, we have

$$\begin{aligned} 1 - \Delta \leq 2\sqrt{\delta} &= 2\sqrt{\tilde{\varepsilon} + \frac{1}{2}\sqrt{2^{1-H^{\tilde{\varepsilon}}_{\min}(X|BC_AC_B)_\rho}}} \\ &\leq 2\sqrt{\tilde{\varepsilon} + \frac{1}{2}\sqrt{2^{1-\ell+n}}} \\ &\leq 2\sqrt{\sqrt{2\varepsilon} + 2^{-\frac{1}{2}(\ell-n+1)}} \end{aligned}$$

where we used the definition of weakly Δ-binding and inequalities (14) and (15). □

Quantum Resource

Next, we consider implementations of string commitments from a functionality which allows the players to commit to (and later reveal) n qubit states. The following theorem shows that there cannot exist a protocol using such a resource which implements an arbitrarily hiding and binding string commitment of length larger than $2n$.

Theorem 15. *Every quantum protocol which uses a resource, which allows the players to commit to (and later reveal) n qubit states and implements an ε-hiding and Δ-binding string commitment of length ℓ must have*

$$\ell \leq 2n - 2\log\left(\frac{(1-\Delta)^2}{4} - \sqrt{2\varepsilon}\right) - 1. \tag{16}$$

In particular, if $\Delta = \varepsilon \leq 0.01$, then $\ell \leq 2n + 6$.

Proof. Let $|x\rangle\langle x| \otimes \rho^x_{ABC}$ be the state resulting from the execution of an ε-hiding commitment protocol when the input of Alice is x. Then $\rho_{XABC} = \sum_x \frac{1}{2^\ell}|x\rangle\langle x| \otimes \rho^x_{ABC}$ is the state resulting from an execution where the committed string X is uniformly distributed. Let $\tilde{\varepsilon} := \sqrt{2\varepsilon}$. Since ρ_{XB} is ε-close to uniform and $P(\rho, \rho') \leq \sqrt{2D(\rho, \rho')}$ [29], the definition of the smooth min-entropy implies that

$$H^{\tilde{\varepsilon}}_{\min}(X|B)_\rho \geq \log |X| = \ell.$$

From Lemma 13 we have

$$H^{\tilde{\varepsilon}}_{\min}(X|BC)_\rho \geq H^{\tilde{\varepsilon}}_{\min}(X|B)_\rho - 2\log|C|. \tag{17}$$

From Lemma 10 we know that there exists a function $f : \{0,1\}^\ell \to \{0,1\}$ such that

$$D(\rho^{\mathcal{X}_0}_{BC}, \rho^{\mathcal{X}_1}_{BC}) \leq 2\delta$$

where $\rho^{\mathcal{X}_z}_{BC} = \frac{1}{2^{\ell-1}} \sum_{x \in f^{-1}(z)} \rho^x_{BC}$ and $\delta := \tilde{\varepsilon} + \frac{1}{2}\sqrt{2^{1-H^{\tilde{\varepsilon}}_{\min}(X|BC)_\rho}}$. Let $z \in \{0,1\}$ and let Alice prepare the state

$$\frac{1}{\sqrt{2^{\ell-1}}} \sum_{x \in f^{-1}(z)} |x\rangle_X \otimes |x\rangle_{X'}$$

and honestly execute the commit protocol with the first half of this state as input. Let $\rho^{\mathcal{X}_z}_{A'BC} = \rho^{\mathcal{X}_z}_{XX'ABC}$ be the resulting state. Then we have $\mathrm{tr}_{\mathrm{A}'}(\rho^{\mathcal{X}_z}_{A'BC}) = \rho^{\mathcal{X}_z}_{BC}$ and, therefore, Lemma 5 implies that there exists a unitary $U_{A'}$ such that

$$D(\tilde{\rho}^{\mathcal{X}_{1-z}}_{A'BC}, \rho^{\mathcal{X}_{1-z}}_{A'BC}) \leq 2\sqrt{\delta} \tag{18}$$

where $\tilde{\rho}^{\mathcal{X}_{1-z}}_{A'BC} = (U_{A'} \otimes \mathbb{1}_{BC})\rho^{\mathcal{X}_z}_{A'BC}(U_A \otimes \mathbb{1}_{BC})^\dagger$. This implies that

$$\begin{aligned} 1 - \Delta \leq 2\sqrt{\delta} &= 2\sqrt{\tilde{\varepsilon} + \frac{1}{2}\sqrt{2^{1-H^{\tilde{\varepsilon}}_{\min}(X|BC)_\rho}}} \\ &\leq 2\sqrt{\tilde{\varepsilon} + \frac{1}{2}\sqrt{2^{1-\ell+2n}}} \\ &\leq 2\sqrt{\sqrt{2\varepsilon} + 2^{-\frac{1}{2}(\ell-2n+1)}} \end{aligned}$$

where we used the definition of weakly Δ-binding and inequalities (17) and (18). □

Note that the proof of Theorem 15 only uses the fact that the resource could be simulated by Bob such that the resulting state at the end of the commit phase is pure conditioned on all the classical communication and the simulated resource uses an additional memory of size at most $\log|C|$. Thus, inequality (16) holds for arbitrary such resources with $\log|C| \leq n$. A simple example of such a resource would be a functionality which generates a tripartite state $|\phi\rangle_{ABC}$ and gives system A to Alice and B to Bob.